程远未来
iFuture Service

□ 机密 □ 秘密

□ 内部 ■ 公开

程远未来
通用分类证书策略

编号：CYWL-I01-2018

版本号：V1.0

重庆程远未来电子商务服务有限公司

发布日期： 2018 年 6 月 29 日

公开

【文档信息】

文档名称	程远未来通用分类证书策略(CP)		
文档编号	CYWL-I01-2018		
关联文档(上级)			
关联文档(下级)	程远未来电子认证业务规则		
保密级别	公开	**文档版本号**	V1.0
制作人	CPS 编写小组	**制作日期**	2018.6.12
复审人	安全策略委员会	**复审日期**	2018.6.27
批准人	安全策略委员会	**批准日期**	2018.6.27
发布人	安全策略委员会	**发布日期**	2018.6.29
受控状态	■是 □否		

【版本变更记录】

生效日期	版本	修改说明	修改人	复审人	批准人
2018 年 6 月	V1.0	创建	徐蕤、刘磊、刘玉祥、李海波、魏薇	安全策略委员会	安全策略委员会

目　　录

1 概括性描述

1.1 概述

证书策略（Certification Policy）是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。电子认证服务机构可以根据需要签发符合一个或多个证书策略的证书。

本证书策略参考互联网标准组织（IETF PKIX 工作组）制定的 RFC3647《Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework》，以及国内标准《GB/T 26855-2011 信息安全技术公钥基础设施证书策略与认证业务声明框架》进行编写。

1.2 文档名称与标识

本文档的名称为《程远未来通用分类证书策略(CP)》，简称《通用分类证书策略》。

1.3 电子认证活动的参与者

1.3.1 电子认证服务机构

电子认证服务机构（Certification Authority）是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。程远未来是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定，依法设立的第三方电子认证服务机构。

1.3.2 注册机构

注册机构（Registration Authority）代表电子认证服务机构建立起证书注册过程，负责受理证书的申请，确认证书申请者（订户）的身份，批准或拒绝证书申请，批准订户的证书撤销请求或直接撤销证书，批准订户的证书更新请求。

1.3.3 订户

订户指从电子认证服务机构或注册机构获得证书的个人、组织机构，即最终用户。订户与电子认证服务机构签署订户协议，接受证书策略的数字证书认证服务，并对证书对应私钥的使用负有法律责任。

1.3.4 依赖方

依赖方是指接受电子认证服务机构的依赖方协议，独立地判断证书策略证书的安全性是否满足其应用的安全需求，并验证本策略证书和相应签名的实体。

1.3.5 其他参与者

其他参与者指除电子认证服务机构、订户和依赖方以外，参与电子认证活动的实体。

1.4 证书应用

1.4.1 适合的证书应用

因为证书标识的主体身份的不同而导致证书应用差异外，订户证书可以广泛应用在电子政务、电子商务、互联网金融及其他社会化活动中，以实现身份认证、电子签名、关键数据加密等目的，同时也确保互联网上信息传递双方身份的合法性和真实性以及信息的完整性和保密性。程远未来的证书分类主要包含以下几类：

1) 个人证书：包括个人身份证书、个人邮件证书等，可用于需要区分、标识、鉴别个人身份的场合，还可用于数据加解密和信息签名，包括订单、合同签名，以实现信息保密，提供信息源发性证明、完整性保障和抗抵赖。
2) 机构证书：包括机构单位证书、机构部门证书、机构职位证书和机构职员证书，可用于需要区分、标识、鉴别机构身份的场合，还可用于数据加解密和信息签名，包括订单、合同签名，以实现信息保密，提供信息源发性证明、完整性保障和抗抵赖。

3) 设备证书：设备证书用于标识终端、服务器、运营设备，还可用于数据加解密和信息签名，以实现信息保密，及提供信息源发性证明、完整性保障。

1.4.2 不适用的证书应用

符合《通用分类证书策略》要求的证书不能在违背相关法律法规规定的情况下使用，不能用于可能直接导致人员伤亡或者严重破坏环境的应用系统。

1.5 策略管理

1.5.1 策略文档管理机构

本《通用分类证书策略》的管理机构是程远未来安全策略委员会。由安全策略委员负责对证书策略进行制订、修订和发布。

1.5.2 联系人

程远未来《电子认证业务规则》在程远未来官方网站发布。

网站地址：http://www.ifutureca.com

电子邮箱：cps@ifutureca.com

联系地址:重庆市渝北区人和街道镜泊中路 5 号远大印务 1 栋 1 层(401121)

电话号码：023-63063149

传真号码：023-63061694

1.5.3 决定 CP 符合策略的机构

本《通用分类证书策略》由程远未来安全策略委员组织制订，报程远未来安全策略委员批准实行。

1.5.4 CP 批准程序

本《通用分类证书策略》由程远未来安全策略委员审批通过后，在程远未来

的官方网站上对外公布，并在对外公布之日起三十日之内向工业和信息化部备案。

1.6 定义和缩写

下列定义适用于本《通用分类证书策略》:

- 公开密钥基础设施（PKI）Public Key Infrastructure

公钥基础设施是一套由硬件、软件、人员、策略和流程构成的，用于生成、管理、分发、使用、存储和撤销数字证书的，利用公钥技术提供安全服务的基础设施。

- 电子认证服务机构（CA）Certification Authority

受用户信任，负责创建和分配公钥证书的权威机构。

- 注册机构（RA）Registration Authority

具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理订户撤销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书。

- 订户 Subscriber

订户是与电子认证服务机构签订协议，接受电子认证服务机构提供的服务的实体。订户应对证书对应的私钥使用负有法律责任。

- 证书主体 Subject

证书主体是证书中的“主体”（Subject）项指明的、持有与证书中载明公钥相对应之私钥的实体。证书主体可以是订户自己，也可以是订户全权控制的设备、账号、域名、IP 地址等。当订户是机构时，证书主体还可以是该机构的下属机构、部门、职员和设备等。

- 证书申请者（也称作证书申请人）Certificate Applicant

证书申请者是指向电子认证服务机构申请证书的个人或机构。证书申请成功后，证书申请者即为订户。

- 证书申请递交人 Certificate Application Deliverer

指向电子认证服务机构或注册机构递交证书申请的自然人，可以是订户或者订户的合法代表。

- 证书策略（CP）Certification Policy

是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

- 电子认证业务规则（CPS）Certification Practice Statement

CPS 是电子认证服务机构在证书生命周期管理过程中所采纳的业务实践的声明。CPS 是对 CP 所宣称内容的一种解释性和支持性文档。

- 密码模块 Cryptography Module

具有安全边界的用于进行密码相关的存储和计算操作的软件或硬件组合。

- 激活数据 Activation Data

用于使密码模块进入可操作状态的数据，可以是口令、生物特征等。

- 依赖方协议 Relying Party Agreement

电子认证服务机构在《电子认证业务规则》或单独载明的与依赖方之间的协议中，规定双方在证书使用和管理过程中所承担的责任和义务。

- 订户协议 Subscriber Agreement

电子认证服务机构与订户所签署的协议，规定了双方在证书使用和管理过程中所承担的责任和义务。

- 数字证书 Digital Certificate

是电子认证服务提供者签发的用以证明证书持有人的电子签名、身份、资格及其他有关信息的电子文件。证书包含有公开密钥拥有者的信息、公开密钥、签名算法、密钥用途和 CA 的数字签名。

- 甄别名（DN，也被称作可辨识名）Distinguished Name

用于标识证书颁发机构和证书主体名称的序列，一般包括国家名称、省名、地理位置、机构名、机构单元名称和通用名称。

- 对象标识符（OID）Object Identifier

对象标识符是一串数字，可以唯一地标识一个对象（例如密码算法、证书策略等）。

- 证书撤销列（CRL）Certificate Revocation List

证书撤销列表是由电子认证服务机构维护的，包含由于各种原因（例如私钥

泄漏、证书中的信息发生改变）在有效期内被撤销的证书的列表，也称证书黑名单。

- CA 撤销列表(ARL) Authority Revocation List

一个经电子认证服务机构数字签名的列表，标记已经被注销的 CA 的公钥证书的列表，表示这些证书已经无效。

- 证书信任链 Certificate Chain

证书信任链是一个用于证书验证的有序证书序列，它包含一个终端订户证书和若干电子认证服务机构证书，证书信任链起始于根证书，终止于终端订户证书。

- 在线证书状态协议（OCSP）Online Certificate Status Protocol

为订户或依赖方提供在线证书状态查询的协议。

- 目录服务（LDAP）Lightweight Directory Access Protocol

轻量级目录访问协议，通常也指符合轻量级目录访问协议的目录服务系统。

- 私钥（电子签名制作数据）Private Key

指在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。私钥是经由数字运算产生的密钥，用于制作电子签名数据，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密。

- 公钥（电子签名验证数据）Public Key

公钥是经由数字运算产生的密钥，用于解密电子签名，确认电子签名人的身份及电子签名的真实性。公钥可以公开，一般标示于在线数据库、存储库或其他公共目录中，使任何希望得到公钥的人都能得到。

- 会话密钥 Session Key

在一次会话中有效地对消息进行加密的密钥，通常为对称算法密钥。

2 信息发布与信息管理

2.1 信息库

电子认证服务机构应建立一个允许公众访问的在线资料库或者使用允许公众访问的在线第三方资料库，并将其签发的证书以及证书状态信息发布到该资料

库上。

2.2 认证信息的发布

电子认证服务机构应将所签发的符合《通用分类证书策略》的证书及其状态信息发布到资料库上，同时还应发布以下文档的最新版本，允许订户或依赖方进行在线查询。

- 证书策略文档
- 《电子认证业务规则》
- 订户协议
- 依赖方协议

2.3 发布时间或频率

电子认证服务机构的相关信息应在生效后及时发布。

《通用分类证书策略》和对应的《电子认证业务规则》的变更，应在审批通过之日起十天内发布。

证书撤销列表应定期签发，或当需要撤销时签发。

2.4 信息库访问控制

公众应可公开访问《证书策略》、《电子认证业务规则》、证书和证书状态信息以及订户协议和依赖方协议。电子认证服务机构应执行控制措施来阻止对资料库信息进行未经授权的添加、删除或修改。

3 身份标识与鉴别

3.1 命名

3.1.1 名称类型

出现在订户证书中的“颁发者”（Issuer）项电子认证服务机构名称和出现

在“主体”（Subject）项的主体名称应采用 X.501 甄别名。

3.1.2 对名称意义化的要求

证书中出现的主体甄别名（DN）应具有一定的代表意义。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

订户不宜使用匿名或伪名。

3.1.4 理解不同名称形式的规则

依 X.501 甄别名命名规则解释。

3.1.5 名称的唯一性

电子认证服务机构不能将主体名称相同的证书签发给不同的订户。电子认证服务机构应具有统一的控制策略，保证每个证书主体拥有唯一的甄别名，同一个订户可能拥有多个相同主体名称的证书。

3.1.6 商标的承认、鉴别和角色

证书申请中包含侵犯第三方知识产权的域名、商标、商号或服务标识的，订户应承担相应的侵权责任。电子认证服务机构不对产权证明材料进行审查。出现产权争端时，电子认证服务机构有权拒绝或挂起引起争端的订户证书申请。

3.2 初始身份确认

3.2.1 证明持有私钥的方法

如果证书私钥在订户一端生成的，证书申请者应证明持有与所要注册公钥相对应的私钥，证明的方法包括在证书请求消息中包含数字签名或其他与此相当的

证明方法。如果密钥对是电子认证服务机构为订户生成的，则不需要进行上述证明，但应测试密钥对的正确性。

3.2.2 机构身份的鉴别

对机构订户鉴别的要求如下：

- 利用政府机构发放的合法性文件（如工商营业执照、组织机构代码证）、权威第三方提供的身份证明或数据库服务，证明该机构的法人身份确实有效存在；
- 通过电话、邮政信函或类似方法确认该机构信息的真实性；
- 确认证书申请递交人得到了证书申请者的明确授权；
- 确认证书申请递交人的合法身份证明并为本人；
- 确认证书主体由证书申请者全权控制。

3.2.3 个人身份的鉴别

对个人订户鉴别的要求如下：

- 利用证书机关发放的合法性文件（如居民身份证）、权威第三方提供的身份证明或数据库服务，证明自然人的身份；
- 通过电话、邮政信函或类似方法确认该个人身份信息的真实性以及代表进行证书申请的个人就是证书申请者本人或是得到了证书申请者的明确授权。

3.2.4 没有验证的订户信息

证书申请递交者提交的非订户身份信息可以不进行验证，如联系地址、电话等。

3.2.5 授权确认

当一个自然人的名称与一个机构名称相关联，可以合法代表机构行使职权时，电子认证服务机构应进行机构的身份鉴别和自然人的身份鉴别并确认该自然人

具有这样的权力。

3.2.6 互操作准则

互操作可能是交叉认证、单身交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的电子认证服务机构之间建立相互信任关系，从而使双方的订户可以实现互相认证。

3.3 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

订户在证书有效期内、且证书未被撤销的情况下提出密钥更新请求，视为常规密钥更新请求。在常规密钥更新时，电子认证服务机构应对订户进行身份鉴别。

3.3.2 撤销后密钥更新的标识与鉴别

订户在证书撤销后申请密钥更新时，需要按照初始证书申请流程重新申请。

3.4 撤销请求的标识与鉴别

订户本人主动发起的证书撤销申请，电子认证服务机构或注册机构应对证书撤销申请人进行身份鉴别，确认撤销申请人是订户本人。

电子认证服务机构或注册机构有充分的理由撤销订户证书的，不需要对订户身份进行标识和鉴别。

司法机关依法提出证书撤销，电子认证服务机构将直接以司法机关书面撤销请求文件作为依据，不再进行其他方式的鉴别。

4 证书生命周期操作要求

4.1 证书申请

4.1.1 证书申请实体

证书申请实体为个人、合法的机构组织。个人订户申请证书时，由其本人或其授权代表申请。机构订户申请机构证书或设备证书时，由机构授权代表申请。

4.1.2 申请过程与责任

证书申请人按照《通用分类证书策略》和《电子认证服务规则》所规定的要求填写证书申请表时，应明确表示同意订户协议中的内容，并提供真实的身份证明材料。如果公私钥由证书申请者自己生成，还应向电子认证服务机构提供相应的公钥，并证明其拥有公钥对应的私钥。

电子认证服务机构或注册机构依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否受理申请。

4.2 证书申请处理

4.2.1 执行识别与鉴别功能

电子认证服务机构或注册机构应根据§3.2 的要求，对证书申请者及证书主体进行身份鉴别。

4.2.2 证书申请批准和拒绝

如果满足下列条件，电子认证服务机构或注册机构将接受证书申请。

- 根据§3.2 的要求，成功的完成了证书的身份鉴别；
- 收到或确认能收到证书申请者需要缴纳的费用。

如果发生下列情形之一，电子认证服务机构或注册机构应拒绝证书申请。

- 证书申请者未能通过身份鉴别；

- 证书申请者不能提供电子认证服务机构需要的补充文件或没有在指定的时间内响应电子认证服务机构的通知；
- 未收到或确认无法收到证书申请者需要缴纳的费用；
- 电子认证服务机构认为批准该申请会将导致电子认证服务机构陷入法律纠纷。

电子认证服务机构或注册机构拒绝申请人证书申请的，应通知申请人，同时向申请人提供失败的原因。

4.2.3 处理证书申请的时限

收到证书申请后，电子认证服务机构或注册机构应当在合理的时限内处理证书申请。

4.3 证书签发

4.3.1 证书签发过程中电子认证服务机构的行为

证书的签发应在证书申请审核通过之后进行。电子认证服务机构产生和签发的证书中的内容应来源于被审核通过的证书申请信息。

4.3.2 电子认证服务机构对订户的通告

电子认证服务机构签发证书后，应及时通知证书申请者，并向证书申请者提供获得证书的方式，确保证书申请者能够通过易于获得的方式获得证书。

4.4 证书接受

4.4.1 构成接受证书的行为

证书申请者按照订户协议中规定的方式确认证书申请者已经接受证书，或者证书申请者在收到电子认证服务机构或注册机构的证书签发通知后在规定时限内未对证书或证书内容提出异议，则认为证书申请者已经接受证书。

4.4.2 电子认证服务机构对证书的发布

电子认证服务机构应将订户已经接受的证书发布到允许公众访问的证书资料库中，并通过可靠的技术手段保障资料库的可用性。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

不作规定。

4.5 密钥对和证书的使用

4.5.1 订户私钥和证书的使用

订户必须在签订了订户协议并接受证书后才能使用证书对应的私钥。订户私钥的使用应符合证书中“密钥用途”(Key Usage）和“增强密钥用途”(Extended Key Usage）的要求。

订户的私钥和证书的使用应符合订户协议的要求。订户应保护其私钥免受未经授权的使用。证书到期或被撤销后，订户应停止使用私钥。

4.5.2 依赖方对公钥和证书的使用

依赖方信任证书的前提是同意依赖方协议中的条款。依赖方应依据证书使用的环境和条件判断证书是否可以信任。如果依赖方需要电子认证服务机构提供额外的保障，依赖方应在确认可以获得这些保障之后信任相应的证书。

在信任证书之前，依赖方应独立的进行如下评估。

- 证书适用于当前的应用场景，并确定证书的使用不违背本证书策略的要求；
- 证书的使用不违背证书中“密钥用途”(Key Usage）和“增强密钥用途”（Extended Key Usage）的规定；
- 证书及其证书信任链中所有电子认证服务机构证书的证书状态是合适的。当证书信任链中的某个证书有被撤销的情况时，依赖方有责任调查上述证书撤销前，订户证书对应私钥所做的签名是否可以信任，并独立

承担相应的风险。

依赖方应利用合适的软硬件来执行数字签名验证或其他密码操作。

4.6 证书更新

4.6.1 证书更新的情形

若证书中的公钥和其他订户信息没有发生任何变化，订户可以通过证书更新获得新证书，过期证书在允许的情形下也可以更新。

4.6.2 请求证书更新的实体

同§4.1.1。

4.6.3 证书更新请求的处理

电子认证服务机构或注册机构对订户证书更新前，应确认证书更新请求是证书订户或订户授权代表提出的，订户应使用拟被更新的证书对应的私钥对更新请求进行签名。

4.6.4 颁发新证书时对订户的通告

同§4.3.2。

4.6.5 构成接受更新证书的行为

同§4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同§4.4.2。

4.6.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3。

4.7 证书密钥更新

4.7.1 证书密钥更新的情形

当订户证书密钥损坏，密钥发生泄露或者其他需要更换密钥的情况发生时，订户可以通过证书密钥更新获得一张包含新公钥、其他订户信息不变的新证书。

4.7.2 请求证书密钥更新的实体

同§4.1.1。

4.7.3 证书密钥更新请求的处理

同§4.6.3。

4.7.4 颁发新证书对订户的通告

同§4.3.2。

4.7.5 构成接受密钥更新证书的行为

同§4.4.1。

4.7.6 电子认证服务机构对密钥更新证书的发布

同§4.4.2。

4.7.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3。

4.8 证书变更

4.8.1 证书变更的情形

当证书中包含的信息（除公钥外）发生变化时，订户可以通过证书变更获得

新证书。

4.8.2 请求证书变更的实体

同§4.1.1。

4.8.3 证书变更请求的处理

证书变更应先对原证书撤销（同§4.9.3），然后按照初始证书申请流程进行处理（同§4.2）。

4.8.4 颁发新证书时对订户的通告

同§4.3.2。

4.8.5 构成接受变更证书的行为

同§4.4.1。

4.8.6 电子认证服务机构对变更证书的发布

同§4.4.2。

4.8.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3。

4.9 证书撤销和挂起

4.9.1 证书撤销的情形

当下列情况之一出现时，应当撤销订户证书，并发布在证书撤销列表中。

- 订户、电子认证服务机构或注册机构有理由相信或怀疑订户证书对应的私钥出现了安全问题；
- 有证据表明订户违反了证书策略、相应的《电子认证业务规则》和订户

协议中的条款或相关法律法规；

- 电子认证服务机构或注册机构有理由相信证书中或者证书申请中的信息是错误的。

4.9.2 请求证书撤销的实体

订户或其授权代表、电子认证服务机构、注册机构、司法机关等公共权力部门可以请求撤销最终用户证书。

4.9.3 撤销请求的流程

电子认证服务机构或注册机构应根据§3.4 的要求，对证书撤销请求人进行身份鉴别。

4.9.4 撤销请求宽限期

证书撤销请求应在发现需要撤销证书情形后的合理时间内提出。该宽限时间应当在《电子认证业务规则》中明确指出。

订户在发现需要撤销证书时，应在当日内发起证书撤销请求。

4.9.5 电子认证服务机构处理撤销请求的时限

电子认证服务机构应在合理的时间内处理证书撤销请求，并在《电子认证业务规则》中对处理时间做出明确规定。

4.9.6 依赖方检查证书撤销的要求

依赖方在信任证书之前，应对证书链上所有证书的状态进行检查，获得证书状态的方法至少应为以下几种方式之一：

- 查询最新的证书撤销列表；
- 通过 OCSP 方式查询；
- 与电子认证服务机构或注册机构约定的其他在线证书查询方式。

依赖方还应对上述证书状态信息的完整性和有效性进行验证。

4.9.7 证书撤销列表的颁发频率

电子认证服务机构应定时签发证书撤销列表。

4.9.8 证书撤销列表发布的最长滞后时间

《电子认证业务规则》应规定证书撤销列表发布的最长滞后时间。

4.9.9 证书状态查询的可用性

至少提供证书撤销列表、在线证书状态协议查询的任意一种，并保证所提供服务的可用性。

4.9.10 撤销信息的其他发布形式

不作规定。

4.9.11 对密钥遭受安全威胁的特别处理要求

如果电子认证服务机构发现或有理由相信其私钥泄露，应立即上报电子认证服务管理部门,并尽可能及时的通知所有订户、潜在的证书依赖方和其他参与方。

4.9.12 证书挂起

不作规定。

4.10 证书状态服务

4.10.1 操作特点

证书状态可以通过电子认证服务机构提供的 WEB 站点、LDAP 目录服务、或者 OCSP 服务获得。

4.10.2 服务可用性

证书状态服务应保证 7*24 小时不间断可用。

4.10.3 可选特征

根据请求者的要求，电子认证服务机构可以提供指定证书的撤销通知服务。

4.11 订购结束

订户出现下列情形时意味着该订户的证书订购已经结束：

- 证书有效期满，订户不再进行证书更新、证书变更或者证书密钥更新；
- 证书有效期内证书被撤销，且订户没有进行证书变更或者证书密钥更新。

4.12 密钥托管与恢复

4.12.1 密钥托管与恢复的策略与行为

电子认证服务机构签名密钥不能托管，其订户的签名密钥托管需满足《中华人民共和国电子签名法》可靠电子签名的要求。

电子认证服务机构可以为订户的加密密钥提供密钥恢复服务，提供密钥恢复服务的电子认证服务机构应在其《电子认证业务规则》中详细描述安全保障措施和服务流程。

4.12.2 会话密钥的封装与恢复的策略与行为

如果电子认证服务机构提供会话密钥封装和恢复服务，应在其《电子认证业务规则》中规定具体的实施流程。

5 电子认证服务机构设施、管理和操作控制

5.1 物理控制

5.1.1 场地位置和建筑

电子认证服务机构的所有操作应在受到物理保护的环境中进行。所采取的物理保护手段应能够保护敏感的信息和系统，防止并检测未经电子认证服务机构授权的访问，使用和披露。

电子认证服务机构应建立多级的物理安全防护区，并对不同安全级别的区域采取不同安全强度的物理防护措施。

电子认证服务机构的区域分级控制应至少四个区域，公共区、服务区、管理区和核心区，发布签名命令的设备以及涉及隐私的资料或数据库需放置在核心区，电子认证服务机构密钥的存储和使用设备需放置在核心区，并进行电子屏蔽。

5.1.2 物理访问

当人员从一个区域进入另一个区域或者进入安全级别较高的区域时，应通过相应的访问控制。

只有授权人员才能对电子认证服务机构的物理设备进行操作。对不同安全区域的访问控制要求如下：

区域名称	访问控制要求
核心区	两人双因素认证 两人以上共同操作
管理区	两人双因素认证 访客需验证身份并登记后方可进入，且有专人陪同
服务区	电子门禁系统
公共区	电子门禁系统

5.1.3 电力和空调

电子认证服务机构的安全设施需要确保电力供应系统保持不间断的电力供应。对于关键的安全设施，需要主、备空调系统来控制温度和湿度。

5.1.4 防水措施

电子认证服务机构的安全设施应安装在具有防水设备的场所，并制定相应的流程，以防止洪水或者其他由于暴露在有水的环境而对系统造成损坏。

5.1.5 火灾预防与保护

电子认证服务机构的设备机房必须提供火灾自动报警系统和应急处理装置，并制定相应的处理流程，以防止明火或者烟雾对电子认证系统造成损害或不利影响。电子认证服务机构的核心区需配备气体灭火装置。

5.1.6 存储介质

电子认证服务机构应保证存储介质不会被意外破坏（如水、火或电磁干扰），不被未经授权的访问。

5.1.7 废弃物处理

电子认证服务机构应制定废弃物处理流程，以安全的方式销毁不再使用的敏感介质、文件和其他废弃物。

5.1.8 异地备份

电子认证服务机构应对关键数据和其他包括审计数据在内的敏感信息提供安全的异地备份。备份中心应设在与生产中心不同的地级行政单位。

5.2 程序控制

5.2.1 关键岗位

关键岗位包括需要访问、操作或者管理认证和密码设备的岗位。

服务于关键岗位的员工被认为是可信人员。参与关键岗位操作的第三方服务人员和顾问等应被认定为“等同可信人员”。

5.2.2 岗位的标识和鉴别

在执行以下操作前，电子认证服务机构应对服务于关键岗位的人员进行鉴别。

- 为可信人员分配用于访问物理设备、设施的权限，并发放实现上述权限所需的门禁卡、指纹录入、钥匙等；
- 为其发放电子凭证，用于访问特定的信息系统和电子认证服务系统。

身份鉴别应包括：由人事职能或安全管理的可信人员对被调查人的身份进行当面的核查，并要求被调查人提供有效身份证件。更进一步的背景调查按照§5.3.2的要求进行。

5.2.3 需要职责分离的岗位

同一个人员不能同时服务于以下任何两个或两个以上的岗位。应进行职责分离的岗位包括但不限于：

- 证书申请信息的鉴别验证；
- 订户信息或者订户请求信息的保管；
- 生成、签发和销毁电子认证服务机构证书；
- 电子认证服务系统的维护。

5.3 人员控制

5.3.1 资历和安全要求

电子认证服务机构应要求可信人员提供有关教育背景、资格证书、相关从业

经历的证明以及无犯罪记录证明。

5.3.2 背景审查流程

电子认证服务机构应制定并执行严格的背景审查流程，对担任关键岗位的人员进行审查，有下列行为的被审查人不能通过审查：

- 被审查人提供虚假信息；
- 有犯罪记录。

5.3.3 培训要求

电子认证服务机构应对其人员进行培训，培训内容与人员对应的职责相关，包括：使用、操作和维护电子认证服务系统过程中涉及的职责、安全机制（例如灾难恢复的方法、业务连续性要求）以及电子认证服务系统的软硬件操作规范等。

电子认证服务机构应定期对培训内容进行审查。

5.3.4 培训周期要求

电子认证服务机构应定期对相关人员进行培训。

当《电子认证业务规则》有重大的内容更新或电子认证服务机构系统有重大的升级改动时，电子认证服务机构应及时对相关人员进行培训。

5.3.5 岗位轮换的频率和顺序

不作规定。

5.3.6 未授权行为的处罚

电子认证服务机构应建立、维护和实施相应的管理办法，对相关人员的未授权行为，如：对电子认证服务系统和资料库等进行的未经授权访问进行处罚，未授权行为出现的次数和严重程度不同，处罚的力度也应不同。

5.3.7 独立合约人的要求

当满足如下条件时，电子认证服务机构可以允许独立合约人或者顾问成为“等同可信人员”：

- 没有合适的雇员能够担当这个岗位的职责；
- 独立合约人或者顾问与雇员具有同等的可信度。

另外，需要访问电子认证服务机构安全设施的独立合约人和顾问，应由电子认证机构的可信人员陪同。

5.3.8 提供给员工的文档

为保障电子认证服务机构运营的规范和安全，电子认证服务机构应确保所有员工能够获得完成工作职责所需的文档，这些文档包括：岗位职责、业务操作说明和电子认证服务机构安全管理的相关规范等。

5.4 审计日志处理流程

5.4.1 应纳入审计记录的事件类型

电子认证服务机构应对审计事件进行记录并审计。所有电子或手工生成的日志都应当包括事件信息、时间和引发事件的实体身份。电子认证服务机构应在《电子认证业务规则》中描述其记录的事件类型。

纳入审计的事件类型包括：

- 对电子认证服务系统的操作事件；
- 证书生命周期事件。
- 可信人员的操作事件。
- 不符合规程的事件。

5.4.2 日志处理周期

电子认证服务机构应对日志进行定期处理，以便发现重要的安全和操作事件。对日志的处理包括：

- 检查日志的完整性。
- 查看日志中的所有记录。
- 分析重要事件的原因并形成总结文档。
- 针对日志中安全记录的事件采取行动，并通过文档记录上述行动。

5.4.3 审计日志的保存期限

审计日志被处理后，在日志生成所在地的保存时间不得少于三年。

5.4.4 审计日志的保护

电子认证服务机构应确保审计日志不被未经授权地访问、复制、修改和删除。

5.4.5 审计日志的备份

审计日志需要定期进行备份。

5.4.6 审计日志收集系统

电子认证服务机构应建立统一的审计日志收集系统，并由专人负责管理。

5.4.7 事件引发主体的通知

不作规定。

5.4.8 脆弱性评估

通过对日志中记录的事件进行审查，对系统的脆弱性进行评估。这种评估需要定期执行，并形成脆弱性评估报告。

5.5 记录归档

5.5.1 归档的记录类型

电子认证服务机构至少需要归档以下记录：

- 所有在§5.4涉及的审计数据；
- 证书申请的相关信息；
- 证书生命周期的相关信息。

5.5.2 归档记录的保存期限

电子认证服务机构的归档记录至少保存五年。

5.5.3 归档记录的保护

电子认证服务机构应采取安全措施，保证未经授权的用户不会浏览、修改和删除电子认证服务机构的归档记录。

归档记录必须采用加密或物理方式进行保护。若采用电子方式进行归档，应采用只读介质。

5.5.4 归档记录的备份流程

电子认证服务机构应对电子和纸质归档记录定期进行异地备份。

5.5.5 归档记录的时间标记要求

电子认证服务机构的归档记录应包含记录产生的时间和日期信息。

5.5.6 归档记录收集系统

电子认证服务机构应该设立内部的档案管理专门机构，统一管理归档记录及其备份。

5.5.7 访问和检验归档记录的流程

只有经授权的可信人员才能访问归档记录。所有归档记录的调用查阅应当记录在案。调用查阅后重新归档时，需验证其完整性。

5.6 电子认证服务机构密钥的更替

电子认证服务机构根密钥的更替，应上报电子认证服务管理部门，并在其监督下重新生成新的密钥，并按照§6.1.4的要求将电子认证服务机构公钥传递给依赖方。

5.7 事故和灾难恢复

5.7.1 事故处理流程

电子认证服务机构应该针对事故的性质制定和实施灾难恢复流程。重大事故需立即上报电子认证服务管理部门。

5.7.2 计算资源、软件和/或数据遭到破坏

电子认证服务机构的计算资源、软件和/或数据等遭到破坏后，电子认证服务机构应采取相应的业务恢复措施。

5.7.3 电子认证服务机构私钥泄露的处理流程

一旦电子认证服务机构的密钥泄露需要被撤销，应立即上报电子认证服务管理部门，并尽可能的通知潜在的依赖方。

5.7.4 灾难发生后的业务连续性

电子认证服务机构应明确灾难发生后的业务恢复时间，用于保证灾难发生后的业务连续性。

5.8 电子认证服务的终止

电子认证服务机构应制定服务终止计划，并在《电子认证业务规则》中公开。

6 认证系统技术安全控制

6.1 密钥对的生成和安装

6.1.1 密钥对的生成

- 电子认证服务机构的密钥生成

电子认证服务机构用于签发证书和证书状态信息的密钥（含根密钥）应由专门的硬件设备生成，生成密钥的系统应能保护私钥不被丢失、泄露、修改和未经授权地访问。

- 订户密钥的生成

订户的密钥对可以由订户、电子认证服务机构或电子认证服务机构委托的机构生成，生成密钥的系统应能保护私钥不被丢失、泄露、修改和未经授权的访问。

由电子认证服务机构或其委托机构生成的订户密钥的传递要符合§6.1.2 的要求。

6.1.2 私钥传送给订户

如果订户自己生成密钥对，则不需要进行私钥传递。

电子认证服务机构或其委托机构代替订户生成私钥，应确保将订户私钥安全的递交给订户。

6.1.3 公钥传送给证书签发机构

订户将自己生成的公钥传递给证书签发机构时，应保证传递方式的安全性，保证公钥的完整性，并证明其拥有公钥对应的私钥。

6.1.4 电子认证服务机构公钥传送给依赖方

电子认证服务机构应当通过安全的途径发布自签名证书或由电子认证服务管理部门发布签名证书。

6.1.5 密钥的长度

密钥算法和长度符合国家密码主管部门的规定。

6.1.6 公钥参数的生成和质量检查

公钥参数应使用国家密码主管部门批准的方式生成和选取，并遵守相应的生成规范和标准。

6.1.7 密钥使用目的

密钥用途应与证书中的“密钥用途”(Key Usage)和“扩展密钥用途”(Extended Key Usage）扩展内容一致。

电子认证服务机构根密钥不能直接用于签发订户证书。

6.2 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

订户可以按照与电子认证服务机构签订的相关协议要求选用密码模块，并妥善保管私钥。

电子认证服务机构所使用的密码模块，应通过国家密码主管部门的专门检测。

6.2.2 私钥的多人控制

对于电子认证服务机构私钥的敏感操作，包括私钥激活、备份和恢复等，应采用多人控制策略，针对同一私钥多人控制策略中的门限值应该是一致的。

订户的私钥由订户自己通过密码模块控制。

6.2.3 私钥托管

电子认证服务机构的私钥不能托管。订户密钥的托管应参照§4.12的要求。

6.2.4 私钥备份

电子认证服务机构的私钥应进行备份，并放置在同等安全程度的场所。电子认证服务机构私钥的备份应由多人控制，要求参照§6.2.2。

电子认证服务机构不对订户的签名私钥进行备份，订户的加密私钥由密钥管理中心备份，备份数据以密文形式存在。

6.2.5 私钥归档

电子认证服务机构的签名私钥在失效后应与密码模块一起进行归档，不能被再次使用。归档的具体要求参见§5.5。

对于订户签名私钥的归档不作规定。

6.2.6 私钥导入或导出密码模块

私钥需要在密码模块中产生，在不同模块之间传输密钥时，需要采用物理的或者密码学手段进行保护，防止私钥丢失、偷窃、修改、泄露或者未经授权的使用。

6.2.7 私钥在密码模块中的存储

电子认证服务机构及其重要组件的私钥需要在密码模块中加密保存。

6.2.8 激活私钥的方法

各参与方应对其私钥的激活数据进行保护，防止丢失、偷窃、修改、泄露或者未经授权的使用。

电子认证服务机构私钥应按照§6.2.2 的要求进行激活。

订户应按照§6.4.1 的要求，在激活私钥之前使用口令或者同等强度的方式进行鉴别。

6.2.9 解除私钥激活状态的方法

电子认证服务机构的私钥在激活后就持续有效，断电将自动解除激活状态。

订户解除私钥激活状态的方法由其自行决定，例如退出、切断电源、移开令牌和自动锁定等。

6.2.10 销毁密钥的方法

当私钥需要被销毁的时候，应按照密码模块给出的说明完成密钥的销毁。

6.2.11 密码模块的评估

密码模块应符合国家密码主管部门的相关规定。

6.3 密钥对管理的其他方面

6.3.1 公钥归档

公钥归档是证书归档的一部分，具体要求参见§5.5。

6.3.2 证书操作期和密钥对使用期限

证书操作周期起始于证书被激活，终止于证书过期或者被撤销。仅用于解密的私钥和用于签名验证的公钥还可能在操作周期后被使用。电子认证服务机构所签发的证书的操作周期不能超过电子认证服务机构密钥对的使用周期。

6.4 激活数据

6.4.1 激活数据的产生和安装

生成和安装私钥激活数据，应采取防护措施来防止私钥丢失、被窃、被篡改、未经授权的披露或者被未经授权地使用。

电子认证服务机构私钥激活数据的生成和安装，应符合§6.2.2 对于多人控制的要求。

订户应使用口令或其他等同安全手段作为激活数据。口令应不易被猜测或能够抵抗字典攻击。

6.4.2 激活数据的保护

各参与方应采取相应的措施保护私钥的激活数据，免受丢失、被窃、被篡改、未经授权的披露或者被未经授权地使用。

电子认证服务机构私钥的秘密分享者不应复制、披露、告知第三方其分享的秘密或对秘密进行未经授权的访问，也不应向第三方透露任何秘密分享者的身份。

6.4.3 激活数据的其他方面

- 激活数据的传递

私钥的激活数据进行传送时，各参与方应保护它们在传送过程中免于丢失、偷窃、修改、未经授权的披露或使用。

- 激活数据的销毁

要求电子认证服务机构保证其私钥的激活数据在销毁的过程中免于丢失、偷窃、未经授权的披露或使用。当超过§5.5.2要求的记录保留期限后，电子认证服务机构应通过覆盖原有记录或者物理销毁的方式来销毁激活数据。

6.5 计算机安全控制

6.5.1 特别的计算机安全技术要求

电子认证服务机构应使用可信的系统来运行软件和存放数据文件，应确保软件和数据不会受到未经授权的访问。

电子认证服务系统应与其他系统进行隔离，只允许已经定义的应用进程对电子认证服务系统进行访问。

为保护电子认证服务机构的网络免受现有攻击的威胁，未使用的端口和服务需要全部关闭。

6.5.2 计算机安全等级要求

不作规定。

6.6 生命周期技术控制

6.6.1 系统开发控制

电子认证服务系统在开发时需要如下的系统开发控制：

电子认证服务软件和硬件在开发时需要有正式的文档化的开发流程支持，购买的商用软件或硬件除外。

电子认证服务机构需要其他专门的软件和硬件的开发环境是可控的，并有正式的文档化的开发流程支持，购买的商用软件或硬件除外。

6.6.2 安全管理控制

电子认证服务机构需要定期对其电子认证服务软件的安全性进行检查。

电子认证服务系统的升级和配置都需要文档化。

软件安装前验证软件的完整性。电子认证服务机构应有相应的机制监视电子认证服务系统的配置变化，并有文档化记录。

6.6.3 生命周期的安全控制

不作规定。

6.7 网络的安全控制

电子认证服务机构应配备网络防火墙、病毒防治、入侵检测、漏洞扫描、数据备份、灾难恢复等安全防护措施。

6.8 时间标记

证书、证书撤销列表、日志和其他关键信息应包含准确的时间和日期信息。

7 证书、证书撤销列表和在线证书状态协议

7.1 证书

CA 签发的证书符合 X.509 V3 格式。遵循 RFC5280 标准。

7.1.1 版本号

版本号为 X.509 V3。

7.1.2 算法对象标识符

符合国家密码主管部门批准的算法对象标识符。

7.1.3 名称形式

命名形式参见§3.1 的要求。

7.1.4 证书扩展项

电子认证服务机构可以根据应用的需要在证书中包含自定义的私有扩展。

7.2 证书撤销列表

电子认证服务机构签发的证书撤销列表符合 X.509 V2 格式。

7.2.1 版本号

版本号为 X.509 V2。

7.2.2 CRL 和 CRL 条目扩展项

CRL 扩展项：颁发机构密钥标识符 Authority Key Identifier。

CRL 条目扩展项：不使用 CRL 条目扩展项

7.3 在线证书状态协议

7.3.1 版本号

使用 OCSP 版本 1（OCSP V1）。

7.3.2 OCSP 扩展项

不使用 OCSP 扩展项。

8 电子认证服务机构审计和其他评估

8.1 评估的频率或情形

电子认证服务机构应接受电子认证服务管理部门组织的定期合规性审计。根据审计结果，需要整改后复审的，电子认证服务机构应接受复审。

电子认证服务机构应定期进行内部审计，审计周期不应长于一年。

8.2 评估者的资质

进行合规性审计和评估的机构，应是电子认证服务管理部门认可的机构。参与电子认证服务机构评估的人员应证明其具备计算机安全方面相关的专业知识，在信息安全和 PKI 审计评估方面有丰富的经验。

内部审计人员由电子认证服务机构内部人员组成。

8.3 评估者与被评估者之间的关系

评估者和电子认证服务机构之间应是相互独立的，没有任何利益关系。

8.4 评估内容

评估包括（但不限于）以下内容：

- 电子认证服务机构是否符合《电子签名法》和《电子认证服务管理办法》

的规定。

- 电子认证服务机构所制定的《电子认证业务规则》是否符合证书策略的要求。
- 电子认证服务机构是否有能力实施其《电子认证业务规则》中制定的相关操作规范和运作协议。

电子认证服务机构是否按照《电子认证业务规则》及相关操作规范和运作协议开展业务。

8.5 对问题与不足采取的措施

电子认证服务机构完成内部评估后，评估人员需要列出所有问题条目的详细清单，由评估人员和被评估对象共同讨论有关问题，并将结果书面通知电子认证服务机构，进行后续处理。

外部评估完成后，电子认证服务机构应根据评估的结果检查缺失和不足，根据提出的整改要求，提交修改和预防措施以及整改计划书，并接受对整改计划的审查，以及对整改情况的再次评估。

对于整改计划不完善或者限期整改后不能达到要求的电子认证服务机构，电子认证服务管理部门有权终止其签发本证书策略体系中证书的服务。

8.6 评估结果的传达与发布

审计评估机构在完成评估后，应向电子认证服务管理部门提交评估结果，电子认证服务管理部门根据需要发布评估结果。

电子认证服务机构内部审计一般不公开评估结果。

9 法律责任和其他业务条款

9.1 费用

9.1.1 证书签发和更新费用

不作规定。

9.1.2 证书查询费用

不作规定。

9.1.3 证书状态查询费用

不作规定。

9.1.4 其他服务费用

不作规定。

9.1.5 退款条件

如果电子认证服务机构违背了证书策略所规定的责任，电子认证服务机构应对订户证书进行撤销并将订户为申请证书所支付的费用全额退还给订户。

关于退款条件的说明，应在《电子认证业务规则》中说明。

9.2 财务责任

电子认证服务机构应拥有足够的财力，以保证电子认证服务的连续性，有能力承担可能出现的对依赖方和订户的赔付。

当订户或依赖方在使用证书过程中造成损失时，电子认证服务机构有义务提供相应的信息，调查损失原因。如果电子认证服务机构不能证明自己无过错，则电子认证服务机构应对终端实体进行赔偿。

9.3 业务信息保密

9.3.1 保密信息

保密信息包括以下内容：

- 电子认证服务机构和订户之间的协议、往来函件等；
- 证书申请材料；
- 审计记录；
- 电子认证服务机构系统操作相关的访问控制信息；
- 电子认证服务机构根据合理的商业判断应理解为保密数据和信息的内容。

除非法律明文规定，电子认证服务机构没有义务公布或透露订户数字证书以外的信息。

9.3.2 非保密信息范围

非保密信息包括（但不限于）以下内容：

- 《电子认证业务规则》；
- 与证书有关的申请流程、手续、申请操作指南等信息；
- 证书、证书撤销列表和其他状态信息。

9.3.3 保护保密信息的责任

任何参与方都有责任保证不泄露保密信息。

9.4 个人隐私保护

9.4.1 隐私保护方案

电子认证服务机构应制定隐私保护方案，保证不会滥用、未经授权使用或出售证书申请者姓名等任何证书申请者资料。电子认证服务机构需要采取必要的安全措施防止证书申请者资料被遗失、盗用和篡改。

9.4.2 视为隐私的信息

除了证书中已经包括的信息外，该订户的其他基本信息和身份鉴别材料，未经订户同意公布的，均视为隐私信息。

9.4.3 不视为隐私的信息

证书申请者提供的用来构成证书内容的信息不被认为是隐私信息。

9.4.4 保护隐私信息的责任

任何接收到隐私信息的参与方有责任保护隐私信息不被泄漏。

9.4.5 使用隐私信息的告知与同意

未得到隐私信息所有者的同意，不得使用隐私信息。

9.4.6 依法律或行政程序的信息披露

依照法律或行政程序进行的信息披露，应当符合下列条件之一：

- 政府法律法规的规定并且经相关部门通过合法程序提出申请；
- 法院以及公共权力部门处理因使用证书产生的纠纷时提出申请；
- 具有合法司法管辖权的仲裁机构的正式申请；
- 证书订户以书面形式进行授权。

9.4.7 其他信息披露情况

其他信息的披露遵循国家的相关规定及与订户的相关协议。

9.5 知识产权

电子认证服务机构保留其签发的证书和证书撤销信息的所有知识产权。任何人可以免费地复制、分发证书和证书撤销列表，只要他们进行完整复制并且证书和证书撤销列表的使用符合相应的依赖方协议。

证书申请者保留证书申请中包含的申请者拥有的商标、服务标志或商业名称以及签发给该证书申请者的证书中可辨识名的所有权利。

9.6 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

电子认证服务机构对签发的数字证书提供的陈述和担保如下：

- 电子认证服务机构在验证和签发证书的时候，不会引入错误信息。
- 所签发的证书满足《通用分类证书策略》的所有要求。
- 撤销服务和资料库的使用符合《通用分类证书策略》的所有要求。

订户协议可以包括额外的陈述和担保。

9.6.2 注册机构的陈述与担保

注册机构是电子认证服务机构的组成部分，其陈述与担保和§9.6.1 是一致的。

9.6.3 订户的陈述与担保

订户提供的陈述和担保如下：

- 订户使用其证书中公钥对应的私钥进行的数字签名是订户认可的数字签名，并且在生成数字签名时，证书已经被订户接受且没有过期或被撤销。
- 订户的私钥受到一定的保护，保证私钥不曾被未经授权的人访问过。
- 在证书申请时，订户提交的所有陈述和信息都是真实的。
- 不将证书和私钥用于非法活动。

订户协议中可以包括额外的陈述和担保。

9.6.4 依赖方的陈述与担保

依赖方认可本证书策略体系中的证书策略，并独立地判断是否依赖证书中的

信息，并对未履行证书策略中规定的依赖方义务而带来的后果承担法律责任。

依赖方协议中可以包括额外的陈述和担保。

9.6.5 其他参与者的陈述与担保

不作规定。

9.7 免责声明

为了特定的商业目的，在法律允许的范围内，各参与方可以通过订户协议、依赖方协议或其他订户协议，对自身的某些义务给予免除。

9.8 赔偿责任限制

电子认证服务机构对由不可抗力，如战争、地震、洪灾、爆炸、恐怖活动等，造成的服务中断并由此造成的客户损失，电子认证服务机构及注册机构不承担责任。

9.9 有限责任

电子认证服务机构在对外服务过程中只承担对外声明的、在《电子认证业务规则》中规定的、对外签署的任何协议中所规定的有限责任。

订户和依赖方的赔偿应在订户协议和依赖方协议中规定。

9.10 赔偿

电子认证服务机构应在其《电子认证业务规则》中规定合理的赔付标准。

9.11 有效期限和终止

9.11.1 有效期限

证书策略自发布之日起生效。

9.11.2 终止

当新版本的证书策略生效时，旧版本的证书策略自动终止。

9.11.3 终止与生存的效力

证书策略终止后，在已签发的证书策略证书的剩余有效期内，证书策略的各条款对各参与方依然具有约束力。

9.12 对各参与者的个别通告与沟通

除非参与方之间另有明确的协议规定，各参与方应根据通信的关键程度和内容，使用商业上合理的方法进行通信。

9.13 修订

9.13.1 修订流程

电子认证服务机构安全策略委员会负责证书策略的修订。

9.13.2 通知机制和期限

电子认证服务机构安全策略委员会保留随时对证书策略进行修订的权利，进行下列（但不限于）不重要的修订后将不作通知：对印刷错误的更正、URL 的改变和联系人信息的变更等。

修订后的证书策略应按照§2.3 的要求及时公布。

9.13.3 应更换对象标识符的情况

不作规定。

9.14 争议处理

出现争议时，按照各参与方签订的协议来处理争端，协商解决不了的问题，可通过法律途径解决。

9.15 管辖法律

证书策略的使用适用于中华人民共和国的法律法规。

9.16 与适用法律的符合性

证书策略的使用也必须遵从使用地的相关法律规定。

9.17 一般条款

9.17.1 完整协议

不作规定。

9.17.2 转让

不作规定。

9.17.3 可分割性

如果证书策略中的任何条款因为某些原因失效或无法执行，证书策略的其他部分仍具有效力。

9.17.4 强制执行

不作规定。

9.17.5 不可抗力

在法律允许的范围内，订户协议和依赖方协议可以包括不可抗力条款。

9.18 其他条款

不作规定。